COMPLIANCE WORK PLAN

Dear Participant,

Welcome to Healthix, the largest public health information exchange (HIE) in New York State and the U.S. Healthix hosts data for over 20 million patients, updated with each encounter. Over 2,000 Participant organizations are connected to Healthix, delivering clinical care from over 8,000 different locations across the New York metro area, including Long Island. Our Participants include large health systems, skilled nursing and long-term care facilities, federally qualified health centers, physician practice groups, community health centers, public health agencies and more.

New York State HIEs (also called RHIOs) are regulated by the New York State Department of Health, in accordance with Article 10 of the New York Code of Rules and Regulations (NYCRR) Part 300. These regulations and corresponding obligations are also outlined in the Statewide Health Information Network of New York (SHIN-NY) guidance, as well as corresponding Healthix Privacy and Security Policies.

Healthix and its Participants must comply with these regulations. To help you better understand your commitment to these regulations and requirements, we have created the **Healthix Compliance Plan.**

The Healthix Compliance Plan includes 7 comprehensive sections. Certain sections have a process for you to follow, which you may have already implemented – in which case, this document will serve to validate your efforts. For others, this document will help you understand requirements and assist in implementing processes and procedures. Several sections will require you to indicate a **point of contact** at your organization, and finally, other sections are purely to provide you with information and to ensure that you understand and will comply with applicable policies. Please be sure to complete the action steps outlined in each section.

The Healthix Compliance Department will designate a Compliance Coordinator who will be your main contact for all matters related to compliance with Healthix Privacy and Security Policies, as outlined in this plan. He or she is always available to answer your questions and to provide continued support to your organization. We look forward to working with you to improve our health care system together.

Sincerely,
Healthix Compliance Team
compliance@healthix.org

Compliance Plan Sections

Organization Full Name: _____

EHR Vendor Name (If applicable): _____

Are you a Covered Entity? [ ] Yes [ ] No

The following sections outline requirements your organization must meet to become a Healthix Participant.

Section 1: Consent Management

Healthix patient consent allows a provider organization (Single Participant Organization) to access patient's data stored by the RHIO to improve and expedite patient's medical care. Healthix provides its Participants with a standardized 2 or 3 option consent form, as applicable:

1.1 Implementation of the Statewide Consent Form:

Single Participant Consent:

1.1- (1) Healthix Participants will use a current version of the consent form required by NYSDOH and attached as ***Exhibit 1A*** or ***Exhibit 1B***

The 3-option consent includes following choices:

(1) Give Consent
(2) Deny Consent unless it is to provide the patient with health care services in a medical emergency only, OR
(3) Deny Consent to access any health information through Healthix for any purpose even in a medical emergency

The 2-option consent includes following choices:

(1) Give Consent
(2) Deny Consent (Note: there is no choice for deny except in an emergency)

1.2 **One-Time Minor Consent:** This consent is applicable to patients ages 10 to under 18 years of age. Minor consent covers access by a practitioner of minor consented services to PHI relating to medical treatment of a minor for which the minor provided his or her own consent without a parent or guardian's permission, as permitted by New York law or other applicable laws for certain types of health services (e.g., reproductive health, HIV testing, STD, mental health or substance abuse treatment) or services consented to by an Emancipated Minor. ***Exhibit 1C***

1.3 **One-to-One Exchange**: A One-to-One Exchange is an agreement between two Participants and Healthix. It allows Healthix to disclose Protected Health Information (PHI) from one **Participant** to another **Participant** for purposes of treatment, quality improvement and/or care management. A One-to-One Exchange is an electronic transfer of information that mirrors a paper-based information exchange such as a referral to a specialist, a discharge summary sent to where the patient is transferred, lab results sent to the ordering provider or clinical information sent from a hospital to the patient's health plan for Quality Improvement or Care Management/Coordination activities. This type of agreement between Participants does not require patients consent; however, all parties are required to sign agreements with Healthix to implement this data sharing. Participants interested in the One-to-One Exchange should contact their Healthix Relationship

Manager or Healthix Customer Support https://healthix.org/techsupport/ for more information. ***Exhibit 1D – 2 Providers, Health Plans***

1.4 Break the Glass Access: Healthix allows one-time only access to a patient's protected health information without the patient or his/her legal representative's affirmative consent in the case of a medical emergency. In this case, the patient has not yet made a consent decision or has opted to deny consent except in an emergency. This is called "Breaking the Glass" (BTG). If a patient has opted to deny consent, then the provider is unable to break the glass, even in an emergency. The following criteria must be met and personally attested to by the individual who is breaking the glass:

1.4-A *An emergency condition exists if, in the individual provider's judgement:*

1.4-A (1) Patient needs immediate medical treatment

1.4-A (2) An attempt to secure consent would result in a delay of treatment, and

1.4-A (3) A delay would increase the risk to the patient's life or health

Only individual users who have been provisioned to have the "BTG" access can "break the glass" – these are usually emergency care providers. It is up to the facility/provider to determine who within their clinical staff would require BTG level access.

1.5 Individual Consent Retention/Storage for Audit: Retain copies of all completed patient consent forms. You may do so electronically or by hard copy, we just suggest that you be consistent. Healthix will need copies of Patient consents when performing our annual Healthix consent audit. The minimal period for retention of the consent forms is six (6) years from the last date of service covered by that consent.

1.6* Withdrawal of Consent:** For patients wishing to withdraw their consent (but not change from one consent decision to another) we require that you implement the following procedure: If a patient wishes to revoke or withdraw an affirmative consent (i.e. change from "Give Consent" or "Deny Consent" to "Undecided"), you must verify the patient's identity, document the request, and notify Healthix immediately by contacting your Healthix Compliance Team member. Please note that withdrawal of the consent, will apply to all dates of service following the date it becomes effective (date of patient's or his/her representative's signed request). ***Exhibit 1E

1.7 Consent Training: All staff responsible for obtaining Healthix patient consent must receive Healthix Consent Training when they first start to collect Healthix consents, and retrained annually, thereafter. If a Participant organization hires new staff, it is their responsibility to provide Healthix Consent Training. Healthix offers in-person group training and "Train the Trainer" sessions. Your dedicated Healthix Compliance Team member will work with you to structure customized training materials. If utilizing a "Train the Trainer" model, Participants need to send Healthix attestation sheets, attached as ***Exhibit 2,*** listing names of the staff who are trained and the dates of training. Please send the attestation to your dedicated Healthix Compliance Team member as soon as the trainings are completed. We request that you identify a point of contact (POC) responsible for working with Healthix to schedule, conduct, and document all trainings.

SECTION 1: ACTION ITEMS

(date and initial that Participant will be in full compliance before Healthix integration project is completed)

1.	Will Implement the Statewide Consent Form	Date	Initials

2.	Which consent option are you implementing: ☐ **2-** option consent OR ☐ **3-** option consent	Date	Initials
3.	Implement Withdrawal of Consent Procedure	Date	Initials
4.	Create & Implement procedure for retaining consent forms	Date	Initials
5.	Train all staff that collect patient consent **before** you begin collecting consent.	Date	Initials
6.	Do you provide minor consented services?	Yes	No

7. Identified Contact for Consent Management

Full Name	Title	Phone #	email

Section 2: Authentication, Authorization, and Access

2.1 Identification of Pilot User: Designate an individual Pilot User to work with the Healthix Project Manager. This person will be set up with a Healthix Portal Account to access the Healthix Clinical Viewer and Clinical Alerts.

2.2 Identification of an Authorized User Manager (AUM): You will also need to designate a contact to request and approve any Healthix Authorized User Accounts. This individual will be responsible for identifying and approving appropriate roles for staff members who utilize Healthix. This individual will also assist with ensuring Healthix Portal Users complete mandatory training modules designated for their assigned roles. This training will be facilitated by Healthix via Litmos. New Users are required to complete training within 30 days of role assignment in order to have access to PHI and complete refresher trainings annually.

2.3 Role Based Access: Identify an individual that will be responsible for working with Healthix to assign each authorized user a role type. ***Exhibit 3A*** contains a table of Healthix user roles.

2.4 NYS I-STOP/PMP User Access: For users who would like to access the NYS I-STOP/PMP – Internet System for Tracking Over-Prescribing must submit access request using ***Exhibit 3B*** form. The individual user or his/her designee will be required to validate information provided to Healthix. The validation should include provider's NPI, NYS License, DEA, and valid and active Health Commerce System (HCS) account.

2.5 Identity Proofing: Verify the identity of *each individual* with whom your organization sponsors and/or validates as an authorized user of Healthix with a valid government issued photo ID, such as a driver's license or passport, and designate an individual that Healthix can contact in the event it needs assistance in confirming the identity of an Authorized User. This function can be performed upon hire or during User Provisioning by the designated Authorized User Manager.

2.6 Change of User Role or Employment Status: Immediately notify Healthix when an Authorized User has been terminated from your employment within **one (1)** business day of termination so that Healthix can disable the individual's access. Some Participants may remove the Authorized User via their Active Directory to disable that individual's access to Healthix. Contact https://healthix.org/techsupport/ to submit request to de-activate a user.

2.7 **Passwords: Passwords shall meet the password strength requirements set forth in NIST SP 800-63 (e.g. the probability of success of an online password guessing attack shall not exceed 1 in 16,384 over the life of the password).

2.8 **Password Change: Authorized User passwords need to change every **90** days.

2.9 **Inactivity of Healthix System: The period of time that the user can keep a session open without entering keystrokes or mouse clicks should not exceed **15 minutes** duration, at which point the application must force log-off.

2.10 **Failed Access Attempts: Require a lock-out and password reset after a **3rd** failed access attempt.**

**Note: These requirements apply ONLY if access to Healthix at your organization occurs through your own EHR or other application (and therefore you set these parameters) -- referred to as "Single Sign On"(SSO).

SECTION 2: ACTION ITEMS

(date and initial that Participant will be in full compliance before Healthix integration project is completed)

1. Identify Pilot User

Full Name	Title	Phone #	email

2. Identify Contact for Identity Proofing

Full Name	Title	Phone #	email

3. Identify Authorized User Manager (AUM)

Full Name	Title	Phone #	email

4. **Confirm adherence to the Single Sign On requirements 2.7-2.10

Date	Initials

Section 3: Patient Engagement

This section will ensure you are prepared to address issues that patients may raise about Healthix and to respond to patient requests. The goal is for your organization to be able to help patients understand what information exists about them, how that information is used, and how they can access it. The "For Patients" section of the Healthix website (www.healthix.org) may be used as a resource to educate and engage patients and consumers.

3.1 **Patient Notice:** It is mandatory to display a patient notice informing patients that your facility is participating in Healthix. The patient notice must be displayed and readily available. The patient notice informs patients that their PHI is being uploaded into Healthix and explains how they may choose to deny consent for all Healthix Participants. Healthix provides a standard patient notice which must be enforced. ***Exhibit 4.***

3.2 **Access to a Patient's own PHI:** Patients are entitled to request copies of their account access audit logs, for up to six years, as well as copies of their medical records. These requests can be filed directly by the patient or via third party application. Please advise the patient to visit Healthix website for more detailed guidance on how to file this request or contact the Healthix Compliance department directly by sending an email to compliance@healthix.org or calling 877-695-4749.

3.3 **Corrections:** Notify Healthix immediately if, in response to a request by a patient, you or the data supplier make any corrections to erroneous patient information. Please send the request to https://healthix.org/techsupport/

3.4 **Restrictions on payers**: Notify Healthix immediately if a patient, who is paying for his/her health services out of pocket, does not want PHI related to those services disclosed to Healthix or any other organization (typically an insurer). Please send the request to https://healthix.org/techsupport/ and include compliance@healthix.org

3.5 **Notify Patients in the event of a Break the Glass access:** If a BTG access occurred during emergency treatment (e.g. an emergency room visit), you are required to notify the patient that their health information was accessed without their consent. The patient is also entitled to ask for a log of the information that was accessed by the provider under these circumstances. This requirement may be satisfied by providing notice, within **10 days**, to all patients who are discharged from your emergency department. You may use Healthix' standard BTG signage ***Exhibit 5*** or you may request approval of a customized notice.

SECTION 3: ACTION ITEMS

(date and initial that Participant will be in full compliance before Healthix integration project is completed)

1.	Display Healthix (RHIO) Patient Notice	Date	Initials
2.	Notify compliance@healthix.org of items 3.2 & 3.3	Date	Initials
3.	Notify Healthix Support https://healthix.org/techsupport/and compliance@healthix.org of items 3.4	Date	Initials
4.	Display BTG Signage, if applicable (otherwise note "N/A")	Date	Initials

5. Indicate the name of the person attesting to completion or acknowledgements as noted above.

Full Name	Title	email

Section 4: Sensitive Data *(if applicable)*

1.	Do you have any SAMHSA/OASAS funded programs?	Yes	No
1a.	*If yes,* will your organization be sending SAMHSA/OASAS data?	Yes	No
2.	Do you have any NYS OMH licensed programs?	Yes	No
2.a	*If yes,* will your organization be sending data from OMH programs?	Yes	No
3.	Do you have any OPWDD licensed programs	Yes	No
3.a	*If yes,* will your organization be sending OPWDD data?	Yes	No

4.1 Identify SAMHSA/OASAS data providing facilities or departments within your organization:

Healthix is required to identify 42 CFR Part 2.11 data contributors within our system. If a federally assisted alcohol or drug treatment program, as defined in 42 CFR Part 2.11, is part of your organization, please help us identify specifically whether that data is being sent to Healthix. Please refer to Definition of a 42 CFR Part 2 program ***Exhibit 6 (a):*** Does Part 2 Apply to Me? *or* ***Exhibit 6 (b)***: How Do I Exchange Part 2 Data?

4.2 Qualified Service Organization Agreement (QSOA): If (1) your organization is a federally assisted drug or alcohol abuse program, or you have identified such a program that is part of your organization, (2) you receive data from such a program, and (3) you may transmit that data to Healthix, federal law requires that you sign a QSOA. A QSOA is a mechanism that allows for the disclosure of information between a 42 CFR Part 2 Program and an organization that provides services to the program, like Healthix. Once a QSOA is in place, federal law permits the Part 2 program to freely communicate information from patients' records to Healthix, **without** patient consent, if it is limited to that information needed by Healthix to provide services to the program. Please refer to ***Exhibit 6 (c)*** for the QSOA form.

4.3 BTG Access of SAMHSA/OASAS data: If your organization is a 42 CFR Part 2 program provider, you must identify a point of contact at your organization that will be responsible for receiving weekly BTG reports. This report will serve to notify you of all instances where your organization's data was accessed through Healthix in a BTG situation. If you have questions regarding BTG reports and how they are distributed, contact compliance@healthix.org– ***Please Note: e-mails must be encrypted*** if they include PHI.

4.4 Programs and services licensed under New York State Office of Mental Health (OMH):

To assure that any information exchanged between Healthix participants complies with NYS Mental Hygiene Law 33.13 (d), Participant must provide accurate validation of any information that will be submitted by the provider to Healthix that is attributable to a program subject to OMH regulations. This exchange of data is specifically related to clinical alerts without patient consent (e.g. "Essential Alerts"). Without a patient's consent, clinical alerts triggered by an encounter at an OMH licensed facility/provider can be shared only with the following providers or entities: (i) Managed Care Organization, (ii) Behavioral Health Organization, (iii) Health Home , (iv) entity specifically approved by the NYS Dept. of Health for purposes of care coordination.

4.5 Programs and services licensed under New York State Office for Persons with Developmental Disabilities (OPWDD):

Healthix must confirm if information exchanged between Healthix participants complies with New York State Mental Hygiene Law Title C - DEVELOPMENTAL DISABILTIES ACT Article 16. As part of the verification process, Participant must provide accurate validation of any information that might be submitted by the provider to Healthix that is attributable to a program subject to OPWDD regulations. This exchange of data is specifically related to clinical alerts without patient consent (e.g. "Essential Alerts"). Without a patient's consent, clinical alerts triggered by an encounter at OPWDD licensed facility/provider can be shared only with the following providers: (i) Managed Care Organization, (ii) Behavioral Health Organization (iii) Health Home , (iv) entity specifically approved by the NYS Dept. of Health for purposes of care coordination.

SECTION 4: ACTION ITEMS

(Date and initial that Participant will be in full compliance before Healthix integration project is completed)

Indicate name of person responsible for identification of the 42 CFR Part 2 programs:

Full Name	Title	Phone #	email

Indicate name of the person designated as the BTG weekly report recipient:

Full Name	Title	Phone #	email

Indicate name of person responsible for identification of the OMH licensed programs:

Full Name	Title	Phone #	email

Indicate name of person responsible for identification of the OPWDD licensed programs:

Full Name	Title	Phone #	email

Section 5: Certified Applications *(if applicable)*

5.1 Work with Healthix to establish your application as a **Certified Application**. A Certified Application is a computer application certified by Healthix that is used by a Participant to access PHI from Healthix on an automated, system to system basis. This means access to Healthix data is managed by the Participant and consequently all its corresponding privacy and security controls. It is imperative to establish, that your system meets minimum-security requirements. Healthix reserves the right to evaluate privacy and security controls through the audit process. ***Exhibit 7(a) and 7(b).***

SECTION 5: ACTION ITEMS

(date and initial that Participant will be in full compliance before Healthix integration project is completed)

1.	Work with Healthix to establish your application as a Certified Application	Date	Initials
Full Name		Title	

Section 6: Audits

New York State Department of Health requires Healthix to perform periodic audits. Periodic audits will be conducted at least on an annual basis. These audits are focused on oversight and management of access to Protected Health Information through Healthix. Audit results are reported to our governing body and may be shared on our public website. All Participants who integrate with and use Healthix services, including those with Certified Applications, are subject to audits.

6.1 Patient Consent: Identify a point of contact that will be responsible for working with Healthix to ensure that your organization completes the state mandated consent audit. You will receive instructions on how the audit will be conducted via email from a member of the Compliance team. You must send Healthix a copy of the consent forms you have stored at your facility for each patient shown in the consent audit list by secure email or Fax. Healthix will evaluate the copies of the consent forms signed by patients. A consent audit report will be generated and shared with your organization. Depending on your audit score, you may be required to perform some remediation. Remediation requirements vary with score ranges.

6.2 User Validation Audit: Identify a point of contact that will be responsible for working with Healthix to ensure that your organization completes the audit. The purpose of the audit is to ensure that the information Healthix has, and the level of access for your authorized users is accurate and up to date. You will receive a report of all your authorized users with active accounts. If necessary, a Corrective Action Plan may be required to address any non-compliance issues identified through the review.

6.3 Identity Proofing: Identify a point of contact responsible for validating your identity proofing process. Healthix will require you to produce documentation for a sample of authorized Healthix users at your organization. Healthix or the Participant must implement initial user identity-proofing procedures (either remote or in person) that require Authorized Users to provide identifying materials and information (e.g., a

valid current primary Government Picture ID and either address of record or nationality, such as a driver's license or passport) upon application for access to information through Healthix.

6.4 User Access Audit: Identify a point of contact that will be responsible for working with Healthix to validate whether the access of the Authorized User was executed appropriately in accordance with SHIN-NY and Healthix policies (example: user involved in direct patient treatment or care management).

6.5 One-to-One (1:1) Exchange: Identify a point of contact that will be responsible for working with Healthix. A Participant in a One-to -One exchange agrees to be audited on a regular basis by Healthix to 1) validate proper authorization between parties, 2) validate patient/member relationship with providers and 3) proper level use of the PHI within the receiving provider.

6.6 Annual HIPAA Training: Confirm that you provide annual HIPAA training to your employees. Healthix reserves the right to request you to produce such documentation, with reasonable notice.

6.7 Office of Civil Rights (OCR) Breach Reporting: Confirm if your facility has reported a breach in the past 24 months. Healthix monitors breaches reported to OCR on a monthly basis. Participants are required to notify Healthix of any breaches of patient privacy. Participants shall notify Healthix in the event that a Participant becomes aware of any actual or suspected Breach involving Protected Health Information accessed via Healthix in accordance with Section 7: Breach, of the Healthix Privacy & Security Policy.

6.8 Break the Glass (BTG): This audit is conducted weekly by the Healthix Compliance Team for all Participants. In cases when there are questions as to whether the BTG access meets Healthix and SHIN-NY policy, the Compliance Team member will contact your facility to investigate the access and to determine a final assessment. These audits apply only to Participants that routinely provide emergency services. If applicable, you will need to identify a point of contact that will be responsible for working with Healthix to ensure that your organization responds to the inquires related to BTG access in a timely manner.

NOTE: *Healthix will continue to develop audits based on New York State DOH mandates. We will assist you in preparation for all audits.*

SECTION 6: ACTION ITEMS

(date and initial that Participant will be in full compliance before Healthix integration project is completed)

1- Identify Contact for Consent Audit

Full Name	Title	Phone #	email

2- Identify Contact for User Validation Audit

Full Name	Title	Phone #	email

3- Identify Contact for Identity Proofing Audit

Full Name	Title	Phone #	email

4- Identify Contact for User Access Audit

Full Name	Title	Phone #	email

5- Identify Contact for **Break the Glass inquiries** (if applicable)

Full Name	Title	Phone #	email

6	Confirm that you/your facility conducts annual HIPAA training.	Date	Initials

7	Has your facility reported a breach to OCR in the past 24 months?	Yes	No

8-**Identify Contact for overall Compliance and Privacy Inquiries**

Full Name	Title	Phone #	email

Section 7: Termination

Termination can be initiated by either party subject to the terms of the Participant Agreement between Healthix and your organization. Termination of the Participation Agreement ends the contractual relationship between your organization and Healthix. It does not discontinue obligations to maintain the privacy and security of patient data under either agreement and/or federal and state law. Your organization's decision to terminate must be communicated to Healthix with minimum of 30-day notice (working days) and must comply with the Healthix Termination Policy and Procedures as well as terms outlined in Participation Agreement and Business Associate Agreement. For more information, please contact your Healthix Relationship Manager, Healthix Customer Support https://healthix.org/techsupport/ or compliance@healthix.org. *Note: If you are the recipient of Data Exchange Incentive Program (DEIP) Funds and cancel before the term stated in the DEIP guidelines, you will be responsible for paying back the New York State Department of Health.*

A. Glossary of Exhibits

Section 1: Consent Management	Exhibit 1A:	Consent Form – With Emergency Services
	Exhibit 1B:	Consent Form – Without Emergency Services
	Exhibit 1C:	Consent Form – Minor One Time Consent
	Exhibit 1D-1:	One-to-One Exchange Form – Two Providers
	Exhibit 1D-2:	One-to-One Exchange Form – Health Plan
	Exhibit 1E:	Consent Withdrawal Form
	Exhibit 2:	Patient Consent Training Attestation
Section 2: Authentication, Authorization, and Access	Exhibit 3A:	Healthix User Roles
	Exhibit 3B:	Healthix I-STOP Access User Request Form
Section 3: Patient Engagement	Exhibit 4:	Participant Participation in HIE Notice
	Exhibit 5:	BTG Signage
Section 4: Sensitive Data (if applicable)		***Definition of a 42 CFR Part 2 program***
	Exhibit 6 (a):	Disclosure of substance Use Disorder Patient Records Does Part 2 Apply to Me?
	Exhibit 6 (b):	Disclosure of substance Use Disorder Patient Records How Do I Exchange Part 2 Data?
	Exhibit 6 (c):	QSOA Form
Section 5: Certified Applications (if applicable)	Exhibit 7(a):	Certified Application Requirements
	Exhibit 7(b):	Certified Application attestation